Implementazione del proxy di autenticazione

Sommario

Introduzione

Il proxy di autenticazione (auth-proxy), disponibile nella versione 12.0.5.T di Cisco IOS® Software Firewall e successive, viene utilizzato per autenticare gli utenti in entrata o in uscita o entrambi. Questi utenti sono in genere bloccati da un elenco di accesso. Tuttavia, con il proxy di autenticazione, gli utenti configurano il browser in modo che ignori il firewall e venga autenticato su un server TACACS+ o RADIUS. Il server comunica al router altre voci dell'elenco degli accessi in modo da permettere il passaggio del traffico dopo l'autenticazione.

Questo documento fornisce all'utente suggerimenti generali per l'implementazione di auth-proxy, fornisce alcuni profili di server Cisco Secure per auth proxy e descrive ciò che l'utente vede quando si usa auth-proxy.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Come implementare il proxy di autenticazione

Attenersi alla seguente procedura:

1. Prima di configurare il proxy di autenticazione, verificare che il traffico scorra correttamente attraverso il firewall.
2. Per ridurre al minimo l'interruzione della rete durante il test, modificare l'elenco degli accessi esistente in modo da negare l'accesso a un client di test.
3. Verificare che un client di test non possa attraversare il firewall e che gli altri host possano passare.
4. Attivare il debug con **exec-timeout 0 0** sulla porta della console o sui terminali virtuali (VTY), mentre si aggiungono i comandi **auth-proxy** e si esegue il test.

Profili server

Il test è stato eseguito con Cisco Secure UNIX e Windows. Se RADIUS è in uso, il server RADIUS deve supportare attributi specifici del fornitore (attributo 26). Di seguito sono riportati esempi specifici di server:

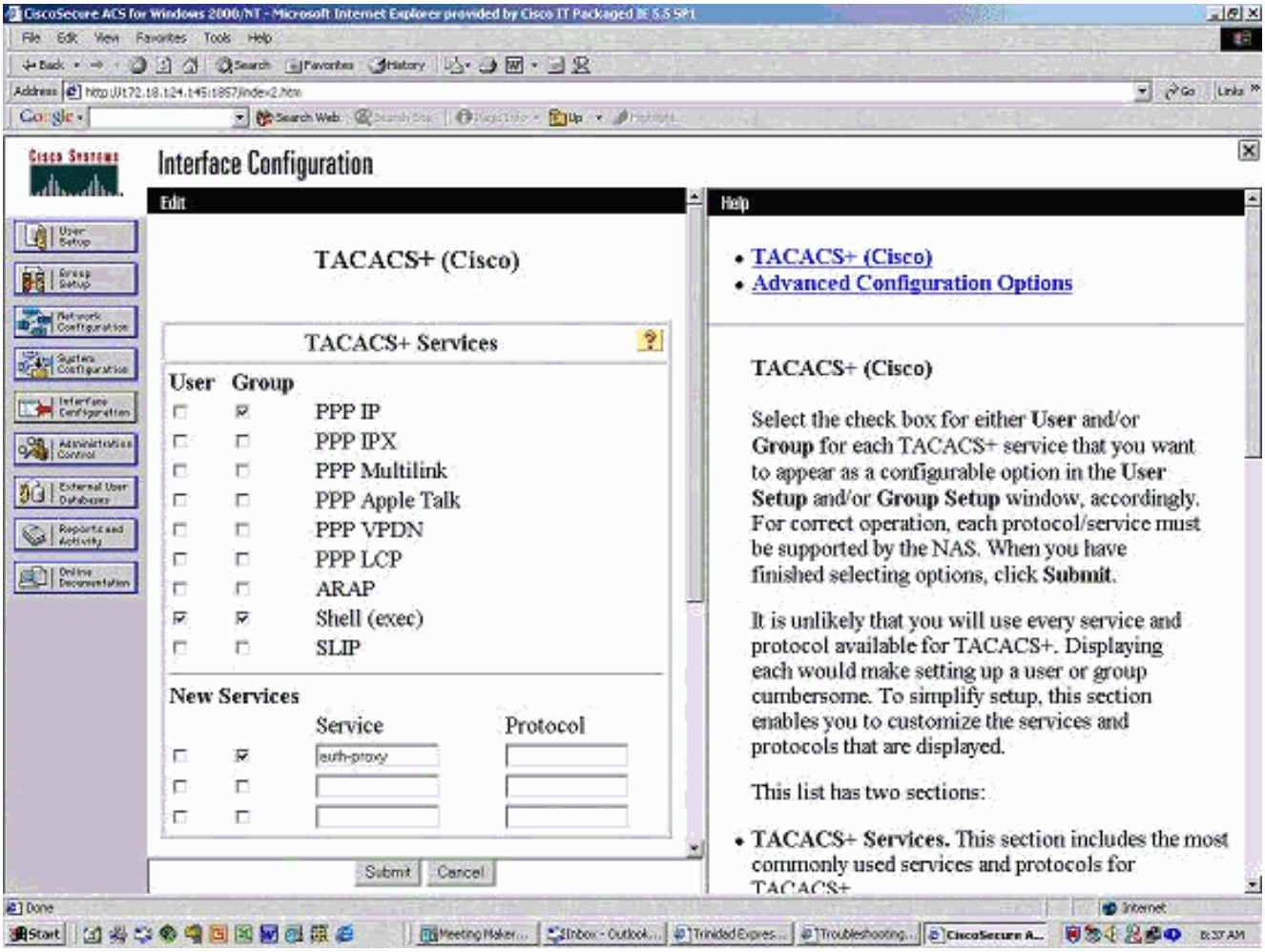
Cisco Secure UNIX (TACACS+)

```
# ./ViewProfile -p 9900 -u proxyonly
User Profile Information
user = proxyonly{
profile_id = 57
set server current-failed-logins = 1
profile_cycle = 2
password = clear "********"
service=auth-proxy {
set priv-lvl=15
set proxyacl#1="permit icmp any any"
set proxyacl#2="permit tcp any any"
set proxyacl#3="permit udp any any"
}
}
```

Cisco Secure Windows (TACACS+)

Attenersi alla procedura seguente.

1. Immettere il nome utente e la password (database Cisco Secure o Windows).
2. Per Interface Configuration (Configurazione interfaccia), selezionare **TACACS+**.
3. In Nuovi servizi selezionare l'opzione **Group** e digitare **auth-proxy** nella colonna Service. Lasciare vuota la colonna
   Protocollo.



4. Avanzate - finestra di visualizzazione per ciascun servizio - attributi personalizzati.
5. In Impostazioni gruppo, selezionare **auth-proxy** e immettere queste informazioni nella finestra:

```
priv-lvl=15
proxyacl#1=permit icmp any any
proxyacl#2=permit tcp any any
proxyacl#3=permit udp any any
```

Cisco Secure UNIX (RADIUS)

```
# ./ViewProfile -p 9900 -u proxy
User Profile Information
user = proxy{
profile_id = 58
profile_cycle = 1
radius=Cisco {
check_items= {
2="proxy"
}
reply_attributes= {
9,1="auth-proxy:priv-lvl=15"
9,1="auth-proxy:proxyacl#1=permit icmp any any"
9,1="auth-proxy:proxyacl#2=permit tcp any any"
9,1="auth-proxy:proxyacl#3=permit udp any any"
}
}
```

}

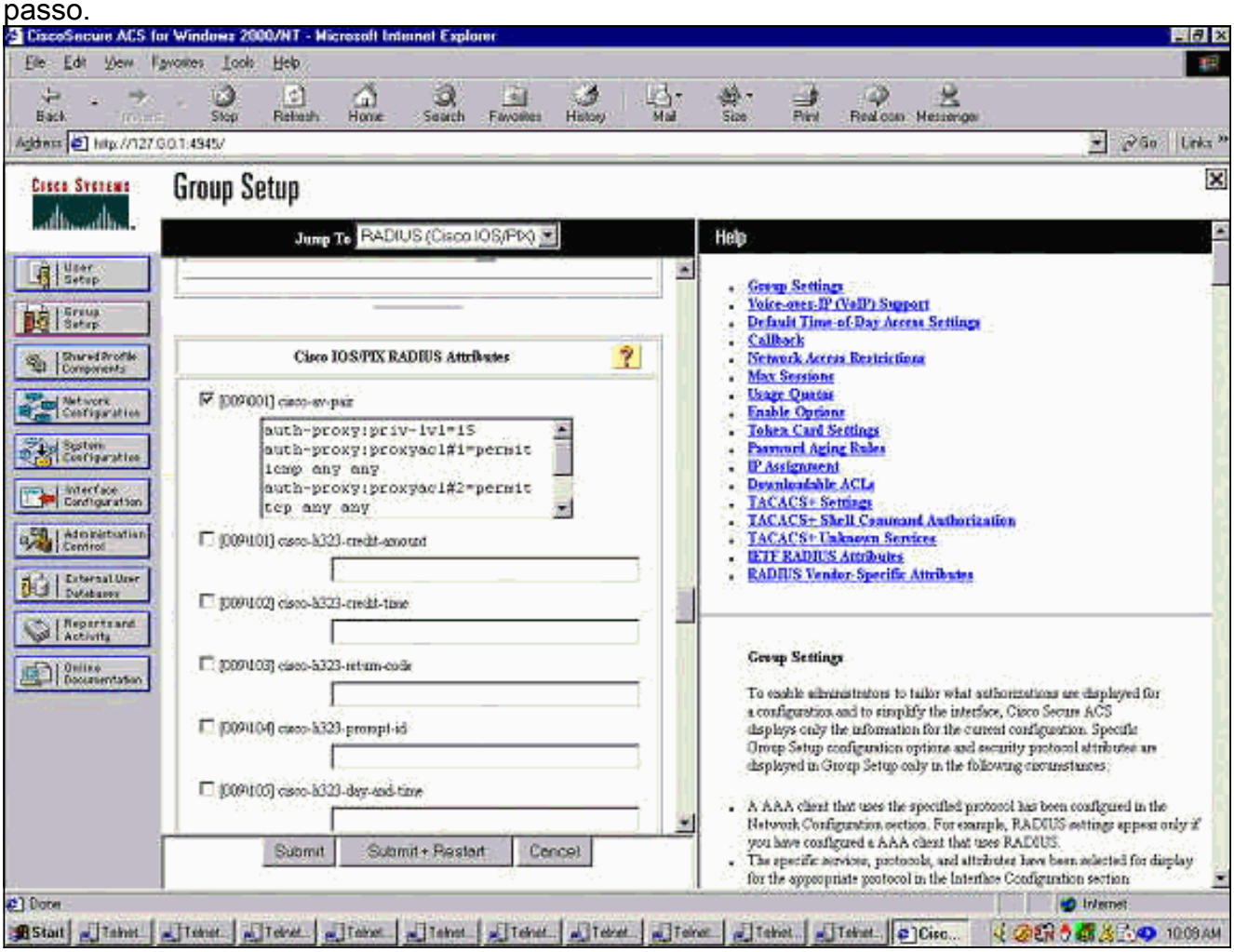
Cisco Secure Windows (RADIUS)

Attenersi alla procedura seguente.

1. Aprire Configurazione di rete. NAS deve essere Cisco RADIUS.
2. Se è disponibile la configurazione interfaccia RADIUS, selezionare le caselle **VSA**.
3. In Impostazioni utente, immettere nome utente/password.
4. In Impostazioni gruppo, selezionare l'opzione per **[009/001] cisco-av-pair**. Nella casella di testo sotto la selezione, digitare quanto segue:

```
auth-proxy:priv-lvl=15
auth-proxy:proxyacl#1=permit icmp any any
auth-proxy:proxyacl#2=permit tcp any any
auth-proxy:proxyacl#3=permit udp any any
```

Questa finestra è un esempio di questo passo.



Cosa vede l'utente

L'utente tenta di sfogliare qualcosa che si trova dall'altro lato del firewall.

Viene visualizzata una finestra con il seguente messaggio:

```
Cisco <hostname> Firewall
Authentication Proxy
Username:
Password:
```

Se il nome utente e la password sono validi, l'utente vedrà:

```
Cisco Systems
Authentication Successful!
```

Se l'autenticazione non riesce, il messaggio è:

```
Cisco Systems
Authentication Failed!
```

Informazioni correlate

- Pagina di supporto di IOS Firewall
- Documentazione e supporto tecnico – Cisco Systems